UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

RONALD STALLONE, on behalf of himself and all other persons similarly situated,

Plaintiff,

vs.

FARMERS GROUP, INC., et al.,

Defendants.

Case No.: 2:21-cv-01659-GMN-VCF

ORDER

Pending before the Court is Defendants Farmers Group, Inc., Farmers Insurance Exchange, 21st Century Insurance Company (collectively "Defendants'") Motion to Dismiss, (ECF No. 21). Plaintiff Ronald Stallone, individually and on behalf of all other similarly situated ("Plaintiff"), filed a Response, (ECF No. 33), and Defendants filed a Reply, (ECF No. 35).

Also pending before the Court is the Motion for Leave to File Supplemental Authority, (ECF No. 32), filed by Defendants. Plaintiff filed a Response, (ECF No. 34), and Defendants filed a Reply, (ECF No. 36).

Similarly pending before Court is the Second Motion for Leave to File Supplemental Authority, (ECF No. 42), filed by Defendants. Plaintiff filed a Response, (ECF No. 47), and Defendants filed a Reply, (ECF No. 48).

Further pending before the Court is the Motion for Leave to File Supplemental Authority, (ECF No. 49), filed by Plaintiff. Defendants filed a Response, (ECF No. 49), and Plaintiff filed a Reply, (ECF No. 51).

///

///

Similarly pending before the Court is the Second Motion for Leave to File Supplemental Authority, (ECF No. 52), filed by Plaintiff. Defendants filed a Response, (ECF No. 53), and Plaintiff filed a Reply, (ECF No. 54).[1]

For the reasons discussed below, the Court **DENIES** Defendants' Motion to Dismiss. Furthermore, the Court **GRANTS** Defendants' Motion for Leave to File Supplemental Authority, and Second Motion for Leave to File Supplemental Authority. Additionally, the Court **GRANTS** Plaintiff's Motion for Leave to File Supplemental Authority and Second Motion for Leave to File Supplemental Authority.

I. BACKGROUND

This case arises from a data breach of Defendants network between January 20, 2021 to February 12, 2021, in which hackers downloaded the personally identifiable information ("PII") of Plaintiff and other similarly situated individuals ("Data Breach").[2] (Am. Compl. ¶ 4, ECF No. 16). Specifically, hackers accessed Plaintiff's driver's license number and address. (*Id*. ¶¶ 7, 21). Defendants operate a single unincorporated business enterprise selling insurance under the service mark "Farmers Insurance Group of Companies." (*Id*. ¶ 11). Defendants' privacy statement on their website states that Defendants "value [their customers] privacy" and that their "policy is to protect the confidentiality of the individually identifiable information . . . and to limit access to that information only to those with a need to know." (*Id*. ¶ 2). Plaintiffs allege that Defendants violated this promise by "readily provid[ing] Plaintiff's and putative

---

[1] The Court may grant leave to file supplemental authority "for good cause" *See* LR 7-2(g). "Good cause may exist when the proffered supplemental authority controls the outcome of the litigation, or when the proffered supplemental authority is precedential, or particularly persuasive or helpful." *Alps Prop. & Cas. Ins. Co. v. Kalicki Collier, LLP*, 526 F. Supp. 3d 805, 812 (D. Nev. 2021). Because the supplemental authority both parties provide in their various Motions to File Supplemental Authority and Second Motions to File Supplemental Authority, (ECF Nos. 32, 42, 49, 52), include published and unpublished federal court cases that are relevant to the issues in this action, the supplemental authority is helpful in developing the Court's analysis.

[2] Pursuant to Rule 23 of the Fed. R. Civ. P., Plaintiff brings this action on behalf of himself and all persons in the state of New York whose PII was compromised as a result of the Data Breach. (*Id*. ¶ 75).

Class Members' driver license numbers to literally *anyone* who entered a person's name, address and/or data of birth into their on-line quoting system." (*Id*. ¶ 3) (emphasis in original).

Plaintiff alleges that this breach was made possible by "Defendants' failure to properly secure their instant quote system, allowing anyone with basic information to obtain drivers' license numbers and other sensitive data." (*Id*.). Hackers were able to obtain Plaintiff's PII from Defendants' online quoting system despite Plaintiff not being a customer of Defendants. (Am. Compl. ¶¶ 7, 19). On April 22, 2021, two to three months after the Data Breach, Defendants notified Plaintiff in a letter that his PII had been compromised. (*Id*. ¶ 23). Defendants' letter encouraged affected individuals to use a free identity theft protection service they offered, and advised those affected to, "[i]n addition to enrolling in Credit Monitoring . . . order your free credit report, place a fraud alert on your credit bureau file, place a security freeze on your credit file and report suspicious activity[.]" (*Id*. ¶ 25). In May 2021, Plaintiff received a letter stating his application for credit at Eddie Bauer was not approved despite never applying for credit. (*Id*. ¶ 24). Plaintiff believes that this denied application was the result of the disclosure of his driver's license number. (*Id*. ¶ 58).

Plaintiff posits he and similarly situated class members now face a heightened long-term risk of future harm, specifically harm posed by identity theft and fraud. (*Id*. ¶ 25, 58). Plaintiff further argues that the dissemination of the PII at issue, namely his driver's license number and address, is significantly more valuable than the loss of other types of PII because driver's license numbers are an integral part of a person's identity and are difficult to change. (*Id*. ¶¶ 32–34). With access to a driver's license number, criminals can fraudulently apply for unemployment benefits. (*Id*. ¶ 35). Moreover, Plaintiff asserts that the PII leaked in the breach will likely be sold or disseminated on the dark web. (*Id*. ¶¶ 26–41). Plaintiff cites sources which show that "personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200." (*Id*. ¶ 31). Plaintiff also provides articles

written by several experts on the monetary value and significance of an individual's driver's license number. (*Id*. ¶¶ 33–35).

Plaintiff contends that Defendants failed to reasonably maintain safety and security measures, especially since insurance companies are frequently targeted by cyber attackers because they work with sensitive data. (*Id*. ¶¶ 42–45). Plaintiff posits that the Data Breach could have been prevented "[h]ad Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the [insurance] field and industry . . . ." (*Id*. ¶ 64). Plaintiff, to mitigate the risk of harm posed by the Data Breach, "review[ed] and monitor[ed] his accounts, enroll[ed] in the free credit monitoring offered, and plac[ed] an alert on his credit with Experian." (*Id*. ¶ 54).

On September 8, 2021, Plaintiff, individually and on behalf of all others similarly situated, filed his first Complaint. (Pl.'s Compl., ECF No. 1). On January 7, 2022, Plaintiff filed the present Amended Complaint, alleging claims for: (1) violation of the Drivers' Privacy Protection Act ("DPPA"), 18 U.S.C. § 2724; (2) negligence; and (3) declaratory and injunctive relief. (Am. Compl. ¶¶ 84–112). On February 8, 2022, Defendants filed the instant Motion to Dismiss. (MTD, ECF No. 21).

II. LEGAL STANDARD

Dismissal is appropriate under Rule 12(b)(6) where a pleader fails to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A pleading must give fair notice of a legally cognizable claim and the grounds on which it rests, and although a court must take all factual allegations as true, legal conclusions couched as factual allegations are insufficient. *Twombly*, 550 U.S. at 555. Accordingly, Rule 12(b)(6) requires "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its

face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* This standard "asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.*

"Generally, a district court may not consider any material beyond the pleadings in ruling on a Rule 12(b)(6) motion." *Hal Roach Studios, Inc. v. Richard Feiner & Co.*, 896 F.2d 1542, 1555 n.19 (9th Cir. 1990). "However, material which is properly submitted as part of the complaint may be considered." *Id.* Similarly, "documents whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the pleading, may be considered in ruling on a Rule 12(b)(6) motion to dismiss." *Branch v. Tunnell*, 14 F.3d 449, 454 (9th Cir. 1994). On a motion to dismiss, a court may also take judicial notice of "matters of public record." *Mack v. S. Bay Beer Distrib.*, 798 F.2d 1279, 1282 (9th Cir. 1986). Otherwise, if a court considers materials outside of the pleadings, the motion to dismiss is converted into a motion for summary judgment. Fed. R. Civ. P. 12(d).

If the court grants a motion to dismiss for failure to state a claim, leave to amend should be granted unless it is clear that the deficiencies of the complaint cannot be cured by amendment. *DeSoto v. Yellow Freight Sys., Inc.*, 957 F.2d 655, 658 (9th Cir. 1992). Pursuant to Rule 15(a), the court should "freely" give leave to amend "when justice so requires," and in the absence of a reason such as "undue delay, bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed undue prejudice to the opposing party by virtue of allowance of the amendment, futility of the amendment, etc." *Foman v. Davis*, 371 U.S. 178, 182 (1962).

III. DISCUSSION

By the instant motion, Defendants seek an order dismissing the above-titled action on the grounds that (1) Plaintiff lacks Article III standing, and (2) that Plaintiff has failed to allege

facts sufficient to support any of his claims for relief. The Court first turns to the question of standing.

Defendants argue that Plaintiff does not have standing before this Court because "Plaintiff's claim of potential future harm, based on the alleged exposure of his driver's license number and address, does not establish an injury in fact." (MTD 12:2–5); *see* (Reply 7:6–17, ECF No. 35). In rebuttal, Plaintiff argues that he has sufficiently alleged four concrete injuries sufficient to confer standing, specifically: (1) an increased risk of identity theft; (2) diminished value of his PII; (3) lost time and expenditures to mitigate the risk of future harm caused by the Data Breach; and (4) additional harm caused by Defendants' delay in notifying Plaintiff of the Data Breach. (Resp. 5:20–25, 12:10–18, ECF No. 33).

The Court evaluates challenges to Article III standing under Fed. R. Civ. P 12(b)(1). *See Maya v. Centex Corp.*, 658 F.3d 1060, 1097 (9th Cir. 2011) (writing that a motion to dismiss for lack of standing is governed by Rule 12(b)(1)). Where, as here, "a defendant in its motion to dismiss under Federal Rule of Civil Procedure 12(b)(1) asserts that the allegations in the complaint are insufficient to establish subject matter jurisdiction as a matter of law (to be distinguished from a claim that the allegations on which jurisdiction depends are not true as a matter of fact), we take the allegations in the plaintiff's complaint as true." *In re Zappos.com, Inc. (Zappos)*, 888 F.3d 1020, 1023 n.2 (9th Cir. 2018) (quoting *Whisnant v. United States*, 400 F.3d 1177, 1179 (9th Cir. 2005).

A. STANDING

"Standing under Article III of the Constitution requires that an injury be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling. *Mosanto Co v. Geerton Seed Farms*, 561 U.S. 139, 149 (2010). Plaintiffs must prove each element with the same manner and degree of evidence required at each stage of litigation. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992). "At the pleading stage,

'general factual allegations of injury resulting from defendant's conduct may suffice." *Mecinas v. Hobbs*, 30 F.4th 890, 897 (9th Cir. 2022) (quoting *Lujan*, 504 U.S. at 561).

In a class action, standing exists where at least one named plaintiff meets these requirements. *Ollier v. Sweetwater Union High Sch. Dist.*, 768 F.3d 843, 865 (9th Cir. 2014). To demonstrate standing, the "named plaintiffs who represent a class must allege and show they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." *Lewis v. Casey*, 518 U.S. 343, 347 (1996) (internal quotation marks omitted). At least one named plaintiff must have standing with respect to each claim that the class representatives seek to bring. *In re Ditropan XL Antitrust Litig*., 529 F. Supp. 2d 1098, 1107 (N.D. Cal. 2007).

In the context of requests for injunctive relief, the standing inquiry requires plaintiffs to "demonstrate that [they have] suffered or [are] threatened with a 'concrete and particularized harm,' coupled with a 'sufficient likelihood that [they] will again be wronged in a similar way.'" *Bates v. Untied States Parcel Serv., Inc.*, 511 F.3d 974, 985 (9th Cir. 2007) (quoting *Lujan*, 504 U.S. at 560). The latter inquiry turns on whether the plaintiff has a "real and immediate threat of repeated injury." *Id*. The threat of future injury cannot be "conjectural or hypothetical" but must be "certainly impending to" constitute an injury in fact for injunctive relief purposes. *Zappos*, 888 F.3d at 1026.

1. Injury-in-Fact

As previously mentioned, Plaintiff argues that he has sufficiently alleged four concrete injuries sufficient to confer standing, specifically: (1) an increased risk of identity theft; (2) diminished value of his PII; (3) lost time and expenditures to mitigate the risk of future harm caused by the Data Breach; and (4) additional harm caused by Defendants' delay in notifying Plaintiff of the Data Breach. (Resp. 5:20–25, 12:10–18). The Court will first examine whether the type of PII released in the data breach exposed Plaintiff to an imminent risk of harm.

a. Cognizable Threat of Future Harm

Defendants argue that under the relevant caselaw, the dissemination of an individual's driver's number and address "is not the type of particularly sensitive personal information that creates a credible threat of fraud or identity theft." (MTD 14:3–7); *see also* (Reply 7:6–9:2). Plaintiff, in rebuttal, asserts that where "a plaintiff alleges facts supporting that the breached data[,]" irrespective of the type of data, "can be used to commit identity theft, it is sufficiently sensitive that a targeted hack to obtain the data creates a 'substantial' risk of identity theft sufficient for Article III injury-in-fact." (Resp. 7:1–6).

Both parties rely on *Krotter v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), and *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018)—the two leading data breaches in the Ninth Circuit that concern standing based on an alleged risk of future identity theft. The hackers in *Krottner* obtained unencrypted names, addresses, and social security numbers, and the *Zappos* hackers obtained names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, full credit card numbers, and unspecified credit and debit card information. *See Zappos*, 888 F.3d at 1023; *Krottner*, 628 F.3d at 1140. The Ninth Circuit in *Zappos* expressly held that "[a] plaintiff threatened with future injury has standing to sue if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." 888 F.3d at 1024 (citation omitted). Based on "the sensitivity of the personal information, combined with its theft," plaintiffs in those cases "adequately alleged an injury in fact supporting standing." *Zappos*, 88 F.3d at 1027. The *Zappos* court also concluded that that the plaintiffs sufficiently alleged standing where their credit card information had been compromised during a data breach, even though there was not indication it had actually been misused. *Zappos*, 888 F.3d at 1027.

Defendant relies on a line of district court cases which have found that the dissemination of an individual's driver's license number and address is not sensitive enough to constitute an

immediate risk of harm. *See Greenstein v Noble Reciprocal Exch.*, 585 F. Supp. 3d 1220, 1227 (N.D. Cal. 2022) (finding that plaintiffs did not establish an imminent risk of harm "because driver's license numbers do not provide hackers with a clear ability to commit fraud"); *In re Uber Techs., Inc., Data Sec. Breach Litig.*, CV 18-2970, 2019 WL 6522843, at *4 (C.D. Cal. Aug. 19, 2019) ("Plaintiff fails to explain how gaining access to one's basic contact information and driver's license number creates a credible threat of fraud or identity theft."); *Antman v. Uber Techs., Inc.*, No. 3:15-cv-01175, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) (Antman I) ("[The plaintiff's] allegations are not sufficient because his complaint alleges only the theft of names and driver's licenses. Without a hack of information such as social security numbers, account numbers, or credit card numbers, there is no obvious, credible risk of identity theft that risks real, immediate injury."); *see also Antman v. Uber Techs., Inc.*, Case No. 15-cv-01175-LB, 2018 WL 2151231, at *10 (N.D. Cal. May 10, 2018) (Antman II) (concluding that the theft of Uber drivers' names and driver's license numbers, combined with bank account and routing numbers, "does not change the court's conclusion that the disclosed information does not plausibly amount to a credible threat of identity theft that risks real, immediate injury"). The Court considers these cases and does not find them persuasive in light of the analysis herein.

The Court finds that "the rightful injury-in-fact determination is not to look at the minutia of what information has been taken — such as credit card information — or social security numbers — but to specifically determine whether the data taken 'gave hackers the means to commit fraud or identity theft.'" *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1034 (N.D. Cal. 2019) (quoting *Zappos*, 888 F.3d at 1027–29)). "The information taken . . . need not be sensitive to weaponize hackers in their quest to commit further fraud or identity theft." *Bass*, 394 F. Supp. 3d at 1034. "Imminent injury in fact can be established through information

similar in function to [a] social security number[ ]," which "derives its value in that it is immutable." *Id*.

As Plaintiff points out, the information compromised in the Data Breach, namely his driver's license number and address, is "difficult and highly problematic" to change. (Am. Compl. ¶ 32). The stolen data here is sufficiently similar to a social security number because it derives its value in large part from its immutability. *Bass*, 394 F. Supp. 3d at 1034. Moreover, Plaintiff has alleged that the Data Breach was part of a targeted campaign in which hackers entered additional PII they already obtained into Defendants online quoting platform to obtain Plaintiff's driver's license number and address. (Resp. 6:1–8); (Am. Compl. ¶ 19). Thus, Plaintiff argues that the Data Breach was part of a concerted campaign by hackers to "pharm" and accumulate the PII of Plaintiff and other victims. (Resp. 7:16–21); (Am. Compl. ¶ 19). Plaintiff cites to multiple experts for the proposition that the PII stolen can, and will likely, be used to fraudulently apply for unemployment benefits, cultivate a fraudulent synthetic identity, or gain access to victim's bank accounts and other personal information. (Am. Compl. ¶¶ 32–34). Thus, the PII stolen here will "provide further ammo" for hackers to commit identity fraud or theft. *Bass*, 395 F. Supp. 3d at 1034.

Hackers targeted Defendants' online quoting platform "with the goal of taking [PII] on a mass scale." *Huyn v. Quora, Inc.*, No. 18-cv-07597, 2019 WL 11502875, at *5 (N.D. Cal. Dec. 19, 2019). "It is not too great a leap to assume, therefore, that their goal in targeting and taking this information was to commit further fraud and identity theft." *Bass*, 394 F. Supp. 3d at 1035. As the United States Court of Appeals for the Seventh Circuit acknowledged, "[w]hy else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015); *see also Galaria v. Nationwide Mut. Ins. Co*., 663 F App'x 384, 388 (6th Cir. 2016).

("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints."). Accordingly, Plaintiff has sufficiently shown that the hacker's intent was not benign, and that the nature of the PII stolen creates a substantial risk of future harm. *See Pygin v. Bombas*, LLC, No. 20-cv-04412, 2021 WL 6496777, at *4 (N.D. Cal. Nov. 29, 2021) (finding that plaintiff had standing where the facts alleged were "sufficient to reasonably infer that the hackers' intent was not benign, and thus, that the Data Breach created a substantial risk of harm" to plaintiff despite plaintiff not showing that his personal information was misused); *see also Huyn v. Quora, Inc.*, No. 18-cv-07597, 2019 WL 11502875, at *5 (N.D. Cal. Dec. 19, 2019) ("Between the obvious goal of taking personal information and the nature and amount of information taken, Plaintiffs have plausibly shown that they are at risk of further fraud and identity theft.").

Additionally, the Court is persuaded that Plaintiff has sufficiently alleged a concrete injury was suffered due to the failed Eddie Bauer credit application. (Am. Compl ¶ 58). Information was stolen, has already surfaced on the Internet, and been misused by others. Given this, the danger that Plaintiffs' data will be subject to further misuse can be described as "certainly impending." *In re Adobe Sys. Privacy Lit.* 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014) (noting that a threatened injury would only be more imminent if information had already been misused). To require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be "literally certain" in order to constitute injury-in-fact. *Id.*; *see also Clapper*, 568 U.S. 398, 414 n.5 (2013). Accordingly, the Court concludes

///

that Plaintiff's allegations of an increased risk of fraud and identity theft are sufficient to establish a credible risk of immediate harm.[3]

b. Diminished Value of PII

Defendants argue that Plaintiff failed to "allege that his [PII] lost value or that he intended to sell his address or driver's license number." (Reply 10:21–23). In rebuttal, Plaintiff contends that the "theft of his driver's license number threatens his license's utility and worth, as a hacker or identity thief of his driver's license numbers can gain access to vehicle registration and insurance policies, as well as access to files kept in doctor's offices and government agencies." (*Id*. 11:17–19).

"Diminution in value of personal information can be a viable theory of damages." *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1234 (D. Nev. 2020), *affirmed* 845 Fed. App'x 613 (9th Cir. 2021). Defendant contends that to show injury in fact under this theory, Plaintiff "must establish both the existence of a market for [his] personal information and an impairment of [his] ability to participate in that market." *Svenson v. Google Inc.*, No. 13-cv-04080, 2016 WL 8943301, at *8 (N.D. Cal. Dec. 21, 2016). Under this formulation of test, a plaintiff must prove that they intended to sell their own PII. *Id*.; *Pruchicki*, 439 F. Supp. at 1235 (examining whether there was specific allegations that plaintiff was "unable to sell" her own PII in assessing any diminution of the value of the PII). These pleading requirements, that a plaintiff must establish both the existence of a market for their PII and an impairment of their

[3] Plaintiff additionally argues that Defendants tacitly admitted that Plaintiff faces an imminent risk of identity theft by offering "identity theft protection and enourag[ing] Plaintiff to use it," and advising him, in addition to enrolling in credit monitoring, to "order [a] free credit report, place a fraud alert on [his] credit bureau file, [and] place a security free on [his] file and report suspicious activity." (Am. Compl. ¶ 25). Likewise, in *Zappos*, the Ninth Circuit considered as evidence of risk of harm the fact that Zappos effectively acknowledged this risk of fraud or identity theft by urging customers to change their passwords. 888 F.3d 1020 (9th Cir. 2018). The Court agrees that Defendant's acknowledgement is a factor to be considered in evaluating the risk of imminent harm. However, this Court is not convinced that this factor alone is dispositive.

ability to participate in that market is not supported by Ninth Circuit precedent, and other district courts in this Circuit have rejected them. *See In re: Anthem, Inc. Data Breach Litig.*, No. 15-md-02617, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) ("These statements [in the case law] appear to require a plaintiff to allege that there was either an economic market for their PII *or* that it would be harder to sell their own PII, not both.") (emphasis in original); *Svenson*¸ 2015 WL 1503429, at *5 ("The Ninth Circuit's holding does *not* require [this] type of explication . . .") (emphasis in original); attack"); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 954 *rev'd on other grounds by In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018) (rejecting plaintiffs' claim that the Zappos security deprived them of the "substantial value" of their personal information where they did not allege they attempted to sell their information and were rebuffed because of a lower price-point attributable to the security breach).

It is undisputed that Plaintiff sufficiently alleged a market for his PII exists on the "dark web." (Am. Compl. ¶¶ 28–34); (Resp. 10:20–23). Defendants' sole argument is that Plaintiff failed to "allege that his information loss value or that he intended to sell his address or driver's license number." (Resp. 10:20–23). However, as explained above, the Court finds that Plaintiff does not have to show that he intended to sell his PII to allege a diminution in value. Therefore, the Court finds that Plaintiff has sufficiently alleged a diminution in the value of his PII.

c. Lost Time & Mitigation Expenditures

Defendants argue that Plaintiff's lost time and mitigation expenses do not constitute an actual injury because Plaintiff has not shown an imminent threat of harm. (MTD 16:3–19). Plaintiff, in response, asserts that because he has shown an imminent threat of harm, his out-of-pocket expenses constitute a cognizable injury-in-fact. (Reply 11:27–12:7).

In *Pruchnicki v. Envision Healthcare Corp.*, the Court held that "tangible, out-of-pocket expenses are required in order for lost time spent monitoring credit to be cognizable as

damages." 439 F. Supp. 3d 1226, 1233 (D. Nev. 2020), *affirmed* 845 Fed. App'x 613 (9th Cir. 2021). While courts have found that credit monitoring may be "compensable where evidence shows that the need for future monitoring is a reasonably certain consequence of the defendant's breach of duty . . . the monitoring must be 'reasonable and necessary.'" *Greenstein*, 585 F. Supp. 3d at 1229–30 (quoting *Corona v. Sony Pictures Entm't, Inc.*, No. 14-cv-09600, 2015 WL 3916744, at *4 (C.D. Cal. June 15, 2015). Thus, courts within the Ninth Circuit have found that out-of-pocket expenses are only warranted when there is an imminent risk of identity theft. *See Stasi v. Immediate Health Grp. Corp.*, No. 19-cv-2353, 2020 WL 2126317, at *9 (S.D. Cal. May 5, 2020) ("Plaintiffs cite no case in which the expenditure of time or money to prevent future identity theft was sufficient in and of itself to support standing without a finding that the threat of identity theft was imminent. Courts addressing the issue have come to the opposite conclusion."); *Antman II*, 2018 WL 2151231, at *10 ("Given this holding [that the threat of identity theft was not imminent] the mitigation expenses do not qualify as injury because the risk of identity theft must be real before mitigation can establish injury in fact."); *Antman I*, 2015 WL 6123054, at *11 ("[M]itigation expenses do not qualify as injury; the risk of identity theft must first be real and imminent, and not speculative, before mitigation costs establish injury in fact."). "Accordingly, for standing purposes, the risk of future identity theft, and the related mitigation costs, are injuries that rise and fall together." *Stasi*, 2020 WL 2126317, at *9.

For the reasons set forth above, the Court finds that Plaintiff has adequately alleged an imminent risk of identity theft. Nevertheless, the Court is not persuaded that Plaintiff has alleged a cognizable injury. Plaintiff contends that following the Data Breach, he "made reasonable efforts to mitigate [the] further impact of the Data Breach, including reviewing and monitoring his accounts, enrolling in the free credit monitoring offered, and placing an alert on his credit with Experian." (Am. Compl. ¶ 54). Thus, Plaintiff does not assert that he spent

additional out-of-pocket mitigation expenses. *See, e.g. Castillo v. Seagate Tech., LLC*, No. 16-cv-01958, 2016 WL 9280242 at *4 (N.D. Cal. Sept. 14, 2016) (finding cognizable injury where some plaintiffs bought a subscription to an identity protection service "because they wanted greater protection than that offered" by the defendant); *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 6333, 650 (N.D. Cal. 2020) (same); *In re Adobe*, 66 F. Supp. 3d at 1217 (same). Instead, Plaintiff merely enrolled in the free credit monitoring service offered by Defendants. (Am. Compl. ¶ 54). Here, the Court declines to recognize enrollment in a free service as an out-of-pocket expense. According to the precedent this Court must follow, Plaintiff's lost time, without an accompanying expenditure, is insufficient to constitute an injury-in-fact.

d. Harm Caused by Defendants' Delay in Notifying Plaintiff

Defendant contends that where "there is no[] imminent threat of harm," mere allegations of delay are insufficient to establish an injury-in-fact. (Reply 10:3–14).[4] Additionally, Defendant argues that Plaintiff failed to articulate how any delay caused harm independent from that caused by the Data Breach itself. (MTD 16:21–17:11). Plaintiff, in rebuttal, asserts that "[w]here, as here, the substantial risk of fraud is established as injury-in-fact, a delay of over two months left Plaintiff and Class Members at an incrementally increased risk because of their inability to start take mitigative steps prior to notification." (Resp. 12:10-18).

To allege a "cognizable injury" arising from delay, a plaintiff must allege "incremental harm suffered as a result of the alleged delay in notification," not merely the data breach itself. *See Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 16-00014, 2016 WL 6523428, at *7 (S.D. Cal. Nov. 3, 2016); *see also In re Sony Gaming Networks*, 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014) ("[A] plaintiff must allege actual damages flowing from the unreasonably delay (and not from the intrusion itself) in order to recover actual damages.").

[4] For the reasons set forth above, the Court finds that Plaintiff has alleged an imminent threat of harm. Therefore, the Court will solely focus on whether Plaintiff adequately alleged an incremental harm caused by delay.

As previously mentioned, Defendant argues that Plaintiff does not allege damages flowing from its months-long disclosure delay. (MTD 16:21–17:11). However, Courts within the Ninth Circuit have found that plaintiffs adequately pled incremental harm when plaintiffs plausibly alleged that they could not take mitigation steps due to defendants delay in notifying them of a data breach. *See In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-02752, 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017) (finding incremental harm was adequately pled in a data breach case when plaintiffs plausibly alleged, they could not take mitigation steps based upon delay); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-cv-2284, 2020 WL 2214152, at *8 (S.D. Cal. May 7, 2020) (same). At this stage in the pleading, the Court assumes as true that had Plaintiff been aware of the Data Breaches a month or two earlier, Plaintiff would have taken earlier measures to mitigate any potential harm suffered from the Data Breach. Defendants' argument is better suited for a motion for summary judgment when the record is more fully developed. Therefore, the Court finds that Plaintiff has plausibly alleged incremental damages arising from Defendants' delay in notifying Plaintiff of the Data Breach.

2. Traceable Injury

Defendant argues that Plaintiff's alleged injuries, including the failed Eddie Bauer application, are not traceable to the Data Breach. (Reply 8:13–9:21). Plaintiff argues that he has shown a traceable injury because there is a logical connection between the Data Breach and the harm suffered by Plaintiff. (Resp. 12:19–28). Specifically, Plaintiff contends that he has sufficiently pled that the Data Breach led to him being exposed to a substantial risk of identity theft, out-of-pocket monitoring costs, lost time, and inchoate harm. (*Id*. 13:1–12).

Here, Plaintiff sufficiently allege that the risk of future "fairly traceable" to the conduct being challenged"—Defendants' failure to prevent the breach. *Lujan*, 504 U.S. at 560–61. As the Ninth Circuit articulated in *Zappos*, "[t]hat hackers might have stolen [p]laintiffs' PII in

unrelated breaches, and that [p]lainitffs might suffer identity theft or fraud caused by the data stolen in those other breaches (rather than the data stolen from Zappos) is less about standing and more about the merits of causation and damages." 888 F.3d at 1029. The *Zappos* court further explained "that 'some other [breach] might also have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue' for the breach in question." *Id.* (quoting *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 696 (7th Cir. 2015))).

Here, the alleged harms are fairly traceable to Defendants because Defendants notified Plaintiff in a letter that he was subject to the Data Breach. (Am. Compl. ¶¶ 23–25); *See Huynh v. Quora, Inc.*, No. 18-cv-07597, 2019 WL 11502875, at *4 (N.D. Cal. Dec. 19, 2019) ("These alleged are fairly traceable to Quora because Quora notified each of the Plaintiffs that they may have been subject of the 2018 Data Breach."). "A reasonable inference can therefore be drawn which traces the plausibly alleged harms to the purported mishandling of [Plaintiff's] personal information through the Data Breach." *Bass*, 394 F. Supp. 3d at 1033. Moreover, as the Ninth Circuit explained, the possibility that some other breach is responsible for causing Plaintiff's PII to be exposed, and correspondingly caused the failed Eddie Bauer application, is "less about standing and more about the merits of causation and damages." *Zappos*, 888 F.3d at 1029. Because the Court assumes, at the pleading stage, that Plaintiff will prevail on the merit of his claim, the Court concludes that Defendants' failure to secure Plaintiff's PII is sufficiently traceable to Plaintiff's alleged injuries.

3. Redressability

Defendants advance two arguments for why Plaintiff lacks standing to seek injunctive and declaratory relief related to requiring Defendants to enhance their security measures. First, Defendants contend that because Plaintiff's PII is leaked no subsequent action taken by Defendants can restore Plaintiff's PII to its pre-Data Breach state. (MTD 18:9–19:8); (Reply

11:19–12:7). Second, Defendants argue that Plaintiff cannot show that there is an imminent risk of another data breach. (MTD 18:9–19:8); (Reply 11:19–12:7). In rebuttal, Plaintiff asserts that he has sufficiently shown that his injuries, namely the substantial risk of identity theft, loss of value of PII, and expenditures mitigating the effects of the Data Breach, are redressable through money damages. (Resp. 13:14–14:5).[5] Additionally, Plaintiff argues that injunctive relief is necessary because it redresses Plaintiff's risk of future harm by preventing ongoing and future violations before the violation occurs. (*Id.* 14:5–15:2).

"[I]t must be 'likely,' as opposed to merely 'speculative,' that the injury will be redressed by a favorable decision." *Lujan*, 504 U.S. at 560–61 (internal quotations and citations omitted). In *TransUnion LLC v. Ramirez*, the Supreme Court explained that "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." 141 S. Ct. 2190, 2210 (2021) (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013); *see also Bates v. United Parcel Service, Inc.*, 511 F.3d 974, 985 (2007) (standing inquiry for injunctive relief requires plaintiffs to "demonstrate that [they have] suffered or [are] threatened with a 'concrete and particularized' legal harm, coupled with a 'sufficient likelihood that [they] will again be wronged in a similar way'").

For the reasons set forth above, the Court finds that Plaintiff has adequately alleged a real and immediate threat of repeated injury from Defendants. Here, hackers were able to obtain Plaintiff's PII from Defendants' online quoting system despite Plaintiff not being a customer of Defendants. (Am. Compl. ¶¶ 7, 19). Plaintiff argues that without injunctive relief

---

[5] The Court agrees with Plaintiff that his alleged injuries are redressable from relief that could be obtained from this litigation. The Ninth Circuit articulated in *Zappos* that plaintiffs injury from the risk of identity theft was redressable because if plaintiffs succeeded on the merits, "any proven injuries could be compensated through damages." 888 F.3d at 1030. Accordingly, all of Plaintiff's alleged injuries could be remedied by money damages. *Id.*

requiring Defendants to remedy the deficiencies in their security measures, Plaintiff's PII could be "obtained again in the same unauthorized manner." (Resp. 14:22–25). Plaintiff therefore faces a "real and immediate threat" of further disclosure of his PII, which remains in the hands of Defendants. *See In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1141 (C.D. Cal. 2021) (writing that plaintiff had standing to pursue injunctive relief where plaintiff asserted that requiring defendants to implement and maintain reasonable security measures was necessary to prevent future data breaches); *In re Yahoo! Inc.*, 2017 WL 3727318, at *31 (finding that plaintiffs had standing to pursue injunctive relief to mitigate the threat of future data breaches when defendants remained in possession of plaintiffs PII); *In re Adobe*, 66 F. Supp. 3d at 1223 (concluding that plaintiff had standing to pursue a declaratory judgment to "prevent future harm from ongoing and future violations before the harm occurs"); *Leonard v. McMemamins*, No. 2:22-cv-00094, 2022 WL 4017674, at **5–6 (W.D. Wash. Sept. 2, 2022) (same). Accordingly, at this stage of the litigation, Plaintiff has adequately alleged standing to seek injunctive and declaratory relief.

For the forgoing reasons, the Court finds that Plaintiff has established standing to pursue his claim. The Court will now examine whether Plaintiff has stated a cognizable DPPA and negligence claim as a matter of law.

B. DPPA

Defendants argue that Plaintiff failed to allege facts sufficient to satisfy the three elements of a DPPA claim. (MTD 19:10–18). In response, Plaintiff posits that he has alleged sufficient facts to state a plausible DPPA claim at this stage in the pleading. (Resp. 16:19–26).

In enacting the DPPA, Congress was motivated by its "[c]oncern[] that personal information collected by States in the licensing of motor vehicle drivers was being released — even sold — with resulting loss of privacy for many persons." *Maracich v. Spears*, 570 U.S. 48, 51–52 (2013) (citing 18 U.S.C. §§ 2721–2725). Consequently, "[t]he DPPA regulates the

disclosure of personal information contained in the records of state motor vehicle departments." *Id*. at 52. To prevail on a DPPA claim, a plaintiff must prove that: (1) defendant knowingly obtained or disclosed his personal information; (2) from a motor vehicle record; (3) for a nonpermissible use. 18 U.S.C. § 2724; *see also Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1257 (9th Cir. 2019). The Court will first examine whether Defendants "knowingly" disclosed Plaintiff's PII.

1. Knowingly

Defendants argue that there was no knowing disclosure of Plaintiff's PIII because the instant quote feature was abused by third parties, and not through any voluntary action taken by Defendants. (MTD 20:15–21:4). Plaintiff, in response, contends that Defendants knowingly disclosed Plaintiff's PIII by configuring an online quoting system which allowed any member of the public to fill in information and receive a quote displaying an individual's driver's license number. (Resp. 17:20–19:15).

A disclosure of PII constitutes a violation of the DPPA only if that disclosure was a "knowing disclosure." 18 U.S.C. § 2724(a). A "knowing disclosure" is a disclosure made voluntarily, not necessarily one made with "knowledge of illegality or potential consequences." *Senne v. Vill. of Palatine*, 695 F.3d 597, 603 (7th Cir. 2012) (en banc); *see In re USAA Data Security Litig.*, No. 21-cv-5813, 2022 WL 3448527, at *7 (S.D.N.Y. Aug, 12, 2022) (applying the definition of "knowing disclosure" used by the Seventh Circuit in *Senne*).

Recently, the United States District Court for the Southern District of New York in *In re USAA Data Security Litig.* found that plaintiffs plausibly alleged that defendant knowingly disclosed their PII under circumstances like the instant action. No. 21-cv-5813, 2022 WL 334852 (S.D.N.Y. Aug. 12, 2022). *In re USAA* involved a data breach of defendant USAA's online quoting platform. *Id*. at *1. To receive a car insurance quote, an individual only had to provide their name, address, and date of birth. *Id*. at *1. After inputting that information, a

USAA member would receive an online quote drawn from the relevant state's department of motor vehicles, including the member's driver's license number. *Id*. at *1. Hackers targeted USAA's online quoting platform and stole plaintiffs' driver's license numbers from the system. *Id*. at *2.

The *In re USAA* court found that Plaintiffs adequately plead a claim under the DPPA. Specifically, the *In re USAA* court found that "USAA's voluntary decision to automatically pre-fill its quote forms with driver's license numbers constitutes a 'knowing disclosure' of personal information." *Id*. at *6 (citing 18 U.S.C. § 2724(a). As in *In re USAA*, the Court finds that Defendants' made a voluntary decision to automatically pre-populate its online quote forms with individuals driver's license numbers upon receiving minimal personal information. Although Defendants were not necessarily aware that this practice would result in the instant Data Breach, the Court finds that Defendants' decision to configure the online quoting platform was a "knowing disclosure" of PII.

2. Motor Vehicle Record

Plaintiff argues he has plausibly alleged that his PII is derived from a motor vehicle record. (Resp. 19:17). Defendants, in rebuttal, argue that Plaintiff's Complaint alleges that his exposed PII came from both motor vehicle records and records outside the purview of the DPPA. (MTD 21:15–26). Therefore, Defendants contend that Plaintiff's allegations are insufficient to show a plausible DPPA claim.

In order to survive a motion to dismiss, a complaint must allege "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft,* 556 U.S. at 678 (internal quotation marks omitted). Here, Plaintiff alleges that his PII originated from motor vehicle records, among other sources. (Am. Compl. ¶¶ 20, 86, 92). Accepting Plaintiff's allegations as true, Plaintiff has plausibly alleged that his PII originated from motor

vehicle records. Defendants' argument is better suited for a motion for summary judgment when the record is more fully developed.

3. Permissible Use

Defendants argue that even assuming there was a disclosure of PII, any disclosure would have been for a permissible use under the DPPA. (MTD 22:1–3); (Reply 15:17–22). Specifically, Defendants contend that the DPPA permits disclosure for insurance rating or underwriting. (MTD 22:12–26); (Reply 15:17–22). Plaintiff, in rebuttal, contends that Defendants cannot maintain that they utilized his PII for insurance rating or underwriting, when Plaintiff neither sought an insurance quote from Defendants nor has he ever been a customer of Defendants. (Resp. 20:21–21:3).

In *Marachich v. Spears*, the Supreme Court spent considerable time discussing the DPPA as a whole, including its exceptions. *See generally* 570 U.S. 48, 65–69 (2013). The Supreme Court advised that the DPPA was to be read narrowly. *Id*. at 60. Specifically, the Supreme Court articulated that although "the DPPA's 14 exceptions permit disclosure of personal information in a range of circumstances," these exceptions "ought not to operate to the farthest reach of their linguistic possibilities if that result would contravene the statutory design." *Id*. Prior federal circuit court decisions reached similar conclusions. *See, e.g.*, *Senne*, 695 F.3d at 603 ("The statute then authorizes specific disclosures — each of which . . . has a limited object and a limited class of recipients.") (second emphasis added); *Thomas v. George, Hartz, Lundeen, Fulmer, Johnstone, King, & Stevens, P.A.*, 525 F.3d 1107, 1114 (11th Cir. 2008) (citing subsection (b)(2) in holding that certain "§ 2721(b) enumerations point to a particularized purpose") (emphasis added). Here, the Court finds that Defendants' interpretation of the applicable DPPA exemption would contravene the statutory design of the DPPA.

///

The DPPA states that information may be disclosed "[f]or use by an insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting." 18 U.S.C. § 2721(b)(6). Defendants claim that under this exemption, any disclosure of PII through its online quoting platform was pursuant to insurance rating or underwriting. (MTD 22:3–26); (Reply 15:16–16:2). Defendants' interpretation takes an expansive view of this exemption. It vests Defendants and other car insurance providers with the absolute discretion to disseminate driver's license numbers on a public forum because it may ultimately facilitate insurance underwriting or rating. This interpretation is difficult to reconcile with the facts of the instant case. Here, hackers were able to obtain Plaintiff's PII from Defendants' online quoting system despite Plaintiff not being a customer of Defendants. (Am. Compl. ¶¶ 7, 19). The DPPA "contains no language that would excuse an impermissible [disclosure] merely because it was executed in conjunction with a permissible purpose." *Pichler v. UNITE*, 542 F.3d 380, 395 (3d Cir. 2008). Therefore, the Court finds that despite Defendants' seemingly permissible purpose, Plaintiff's have plausibly alleged that the online quoting platform produced an impermissible disclosure of PII.

Accordingly, the Court finds that Plaintiff's DPPA claim may proceed.

C. NEGLIGENCE

As a preliminary matter, Defendants argue that Plaintiff's negligence claim should be dismissed because Plaintiff fails to identify which state's law applies. (MTD 23:3–4). In rebuttal, Plaintiff contends that this is a requirement in "California courts, not Nevada." (Resp. 22:26–28).

United States District Courts in California have found that the failure to identify which state law governs warrants dismissal of the claim. *See In re Samsung Galaxy Smartphone Mktg. & Sales Practices Litig.*, No. 16-06391, 2018 WL 1576457, at *4 (N.D. Cal. Mar. 30, 2018)

("As this Court and other courts in this district have recognized, 'due to variances among state laws, failure to allege which state law governs a common law claim is grounds for dismissal.'" (quoting *In re Nexus 6P*, 293 F. Supp. 3d 888, 933 (N.D. Cal. 2018*); In re Static Random Access Memory (SRAM) Antitrust Litig*., 580 F. Supp. 2d 896, 910 (N.D. Cal. 2008) (dismissing an unjust enrichment claim because "until plaintiffs indicate which [s]tates' laws support their claim, the Court cannot assess whether the claim has been adequately [pled]"). This is because "[e]ven if the basic elements of the [common law claims] are unlikely to differ much from state to state, 'there may be (and likely are) differences from state to state regarding issues such as applicable statute of limitations and various equitable defenses.'" *Mendez v. Glob. Inst. of Stem Cell Therapy and Rsch., USA*, No. 20-cv-915, 2022 WL 3019858, at *4 (S.D. Cal. July 29, 2022) (citation omitted).

Here, the Court find Defendants' lack of specificity argument in favor of dismissal is not persuasive. This argument has not been adopted by district courts outside of California, including in any prior decision of this Court. Accordingly, the Court will address whether Plaintiff has alleged a cognizable negligence claim.

Defendants additionally argue that Plaintiff's negligence claim fails as a matter of law because he has not adequately plead causation and damages. (MTD 24:3–14). Plaintiff, in rebuttal, argues that he has alleged damages in the form of the risk of identity theft, loss of value of PII, out-of-pocket costs, and lost time that were caused by Defendants. (Resp. 22:17–24:21).

Under Nevada law, "[t]o prevail on a negligence claim, a plaintiff must establish four elements: (1) the existence of a duty of care, (2) breach of that duty, (3) legal causation, and (4) damages." *Sanchez ex rel. Sanchez v. Wal-Mart Stores, Inc.*, 125 Nev. 818, 824 (2009).

Here, the Court finds that Plaintiff has sufficiently alleged causation and damages. Foremost, Defendants notified Plaintiff in a letter that he was subject to the Data Breach. (Am.

Compl. ¶¶ 23–25). *See Huynh v. Quora, Inc.*, No. 18-cv-07597, 2019 WL 11502875, at *4 (N.D. Cal. Dec. 19, 2019) ("These alleged are fairly traceable to Quora because Quora notified each of the Plaintiffs that they may have been subject of the 2018 Data Breach."). "A reasonable inference can therefore be drawn which traces the plausibly alleged harms to the purported mishandling of [Plaintiff's] personal information through the Data Breach." *Bass*, 394 F. Supp. 3d at 1033. Moreover, for the reasons set forth above, the Court finds that Plaintiff has sufficiently alleged damages due to the diminished value of his PII.[6] Accordingly, the Court finds that Plaintiff has alleged a cognizable negligence claim.

The Court will now address whether Plaintiff's declaratory relief claim may stand as its own cause of action and is not merely a prayer for relief.

D. DECLARATORY AND INJUNCTIVE RELIEF

Defendants move to dismiss Plaintiff's request for declaratory and injunctive relief because "they are requests for remedies—not independent causes of action." (MTD 27:22–23). In response, Plaintiff posits that injunctive and declaratory relief are valid independent causes of action which are necessary to require Defendants to implement additional security measures to prevent future data breaches. (Resp. 24:24–25:9).

Under 28 U.S.C. § 2201(a), "any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking declaration, whether or not further relief is or could be sought." The Declaratory Judgment Act "does not create new substantive rights, but merely expands the remedies available in federal courts." *Shell Gulf of Mexico Inc. v. Ctr. for Biological Diversity, Inc.*, 771 F.3d 632, 635 (9th Cir. 2014). "That is not to say that a claim for declaratory relief may never stand on its own." *V5 Techs., LLC v. Switch, Ltd.*, No. 2:17-cv-2349, 2019 WL 13157438, at *1

[6] Because the Court finds that Plaintiff sufficiently alleged a diminution in the value of his PII, it does not address Plaintiff's other theories of damages.

(D. Nev. Sept. 25, 2019). To survive on its own, a claim for declaratory relief must be justiciable, and the Court must have jurisdiction. *Shell Gulf of Mexico Inc*., 771 F.3d at 635. A claim for declaratory relief may be "unnecessary where an adequate remedy exists under some other cause of action." *Reyes v. Nationstar Mortg. LLC*, No. 15-cv-01109, 2015 WL 455377, at *7 (N.D. Cal. July 28, 2015).

Based on the pleadings, Plaintiff's negligence claim seeks a different relief than his claim for injunctive and declaratory relief. The negligence claim requests retrospective relief — namely, damages — for the past harms that Plaintiff have suffered as a result of Defendants' failure to keep their promises about adequate security. (Am Compl. ¶¶ 89–103). In contrast, the injunctive and declaratory relief claim asks the Court to declare that Defendants must implement additional security measures to prevent the possibility of future data breaches. (*Id.* 104–112). Therefore, the Court concludes that Plaintiff's injunctive and declaratory relief claim appears to serve a distinct purpose from the negligence claim and thus should not be dismissed.

///

///

///

///

///

///

///

///

///

///

///

///

///

IV. CONCLUSION

IT IS HEREBY ORDERED that Defendants' Motion to Dismiss, (ECF No. 21), is **DENIED**.

IT IS FURTHER ORDERED that Plaintiff may file an amended complaint within twenty-one days of this order.

IT IS FURTHER ORDERED that Defendants' Motion for Leave to File Supplemental Authority, (ECF No. 32), is **GRANTED**.

IT IS FURTHER ORDERED that Defendants' Second Motion for Leave to File Supplemental Authority, ECF No. 42), is **GRANTED**.

IT IS FURTHER ORDERED that Plaintiff's Motion for Leave to File Supplemental Authority, (ECF No. 49), is **GRANTED**.

IT IS FURTHER ORDERED that Plaintiff's Second Motion for Leave to File Supplemental Authority, (ECF No. 52), is **GRANTED**.

DATED this 15 day of October, 2022.

Gloria M. Navarro, District Judge
UNITED STATES DISTRICT COURT